Data Protection Policy

ODBST Level 1 Policy:	**ALL** Schools require this policy with **no changes** allowed to core text. No changes are necessary to personalise this with school name and branding, as this is a Trust level policy for use, without change, by all schools, **except** where a school contact is required as identified in the content of the policy. LGBs will **note** adoption in LGB meetings. Review will take place at Trust level, and schools will be notified of updates and review dates as necessary.
Other related ODBST policies and procedures:	Record Management Policy And Annual Review of School Records and Safe Data Destruction Checklist
Committee responsible:	FRAPP
Approved by:	FRAPP/Trust board
Date Approved:	11th July 2023
Review Date:	Summer term 2024

In reviewing this policy the Trust Board has had regards to the Equality Act 2010 and carried out an equality impact assessment. It is satisfied that no group with a protected characteristic will be unfairly disadvantaged

Data Protection Policy

Contents

Data Protection Policy

1. Aims

The Oxford Diocesan Bucks Schools Trust (ODBST) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation & Guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

If the School uses CCTV: It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.
In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The Trust, through its schools, processes personal information relating to parents, pupils, staff, governors, visitors and others and is therefore a data controller. The Trust delegates the responsibility of data controller on a day-to-day basis to the Chief Operating Officer of the Trust. The Trust is registered as a data controller with the Information Commissioner's Office and will renew this registration annually or as otherwise legally required.

Data Protection Policy

Roles & Responsibilities

This policy applies to **all staff** employed by ODBST, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Local Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the trust board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO's contact details are below:

ODBST Data Protection Officer
Rachael Hollinshead
Oxford Diocesan Bucks Schools Trust
The Green
Longwick
Buckinghamshire
HP27 9QY

Email: admin@odbst.org

Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether they have a lawful basis to use personal data in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

5. Data Protection Principles

The GDPR is based on data protection principles that our Trust and schools must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

6. Collecting Personal Data

a. Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law**. Limitation, minimisation and**

accuracy.

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the ODBST Records Management Policy and Annual Review Checklist.

7. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

8. Subject Access Requests and other Rights of Individuals

a. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the trust or school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO using the Trust template. (See Appendix 3) They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

b. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 (Primary School):
Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above (Secondary School):
Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

c. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made

- Will provide the information free of charge
- Will respond without delay and within 1 month (30 days including weekends) of receipt of the request, except in circumstances where a request is complex or numerous, in which case we may inform the individual that we will comply within 3 months of receipt. We will inform them of this within 1 month of receipt and explain why this extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

d. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9. Parental requests to see Educational Record

The ODBST policy for academies is that whilst not legally required, in a similar way to maintained schools, we give the right for free parental access to their child's educational record (which

includes most information about a pupil) within 15 school days of receipt of a written request.

10. Biometric Recognition Systems

If and where the School uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). If a biometric system is introduced, we will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in a school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

11. CCTV

The Trust or School may use CCTV in various locations around its sites to ensure it remains safe. If we use CCTV we will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Data Protection Officer.

12. Photographs & Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Pupils aged under 18 years of age:
We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Pupils aged 18 years and over:
We will obtain written consent directly from pupils aged 18 and over, or their parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within the trust on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of trust by external agencies such as the school photographer, newspapers, campaigns
- Online on our trust or school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

13. Data Protection by Design & Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data Security & Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office. Eg pupil/staff files
- Passwords that are at least 8 characters long containing letters and numbers are used to access trust/school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices where personal information is stored
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for trust/school-owned equipment (see our E-Safety policy on acceptable use)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the trust/school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal Data Breaches

The trust and school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when any changes are made to the bill that affect our trust's practice. Otherwise, or from then on, this policy will be reviewed annually and shared with the full Trust board.

19. Links with Other Policies

This data protection policy is linked to other policies including:

- Freedom of Information Policy (Including publication scheme)

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO in writing about the event using the Data Breach template (see Appendix 4.).
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO on the Trust's central systems.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored by the DPO on the Trust's central systems.
- The DPO and headteacher will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the school on behalf of the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The school on behalf of the DPO will ensure ODBST receive a written response from all the individuals who received the data, confirming that they have complied with this request. The DPO will check this has happened
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website

- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

Appendix 2 – Model Privacy Notices

1. Privacy notice for parents/carers

Privacy Notice For Parents / Carers of Pupils attending XXXXX School

XXXXX School collects data and information about parents / carers of our pupils so that we can operate effectively as a school. This privacy notice explains how and why we collect parent / carer data, what we do with it and what rights parents have.

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth certificate or has parental responsibility for the pupil, with whom the pupil lives or whether the pupil has contact with that parent), and also includes non-parents who have parental responsibility for the pupil, or with whom the pupil lives. It is therefore possible for a pupil to have several "parents" for the purposes of education law. This privacy notice also covers other members of pupils' families who we may process data about from time to time, including, for example, siblings, aunts and uncles and grandparents.

Privacy Notice (How we use parent / carer information)

XXXXX School is part of the Oxford Diocesan Bucks Schools Trust (ODBST). ODBST are the 'data controller' for the purposes of UK data protection law.

Any queries about this notice should be addressed to either the Headteacher, xxxxxx, the Office Manager, xxxx, or our Data Protection Officer (DPO), Mrs Rachael Hollinshead. They can be contacted via the school office on xxxxx or by email via admin@odbst.org

Why do we collect and use parent / carer information?

We collect and use parent / carer information under the following lawful bases:

a. where we have the consent of the data subject (Article 6 (a))
b. where it is necessary for compliance with a legal obligation (Article 6 (c))
c. where processing is necessary to protect the vital interests of the data subject or another person (Article 6(d))
d. where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (e))

Where the personal data we collect about parents / carers is sensitive personal data, we will only process it where:

a. we have explicit consent;
b. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; and / or
c. processing is necessary for reasons of substantial public interest, on the basis of Union or Member

State law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Please see our Data Protection Policy for a definition of sensitive personal data.

We use the parent / carer data to support our functions of running a school, in particular:

a. to decide who to admit to the school;
b. to support pupil learning;
c. to monitor and report on pupil progress;
d. to provide appropriate pastoral care;
e. to administer admissions waiting lists
f. to conduct research
g. to assess the quality of our services;
h. to comply with the law regarding data sharing;
i. for the protection and welfare of pupils and others in the school, including our safeguarding / child protection obligations;
j. for the safe and orderly running of the school;
k. to promote the school;
l. to send you communications that may be of interest to you which may include information about school events or activities, news, campaigns, appeals, other fundraising activities;
m. in order to respond to investigations from our regulators or to respond to complaints raised by our stakeholders;
n. in connection with any legal proceedings threatened or commenced against the school.

The categories of parent / carer information that we collect, hold and share include:

a. Personal information (such as name, address, telephone number and email address);
b. Information relating to your identity, marital status, employment status, religion, ethnicity, language, medical conditions, nationality, country of birth and free school meal / pupil premium eligibility / entitlement to certain benefits, national insurance numbers, information about court orders in place affecting parenting arrangements for pupils);
c. Child protection information
d. Photographs and CCTV images

From time to time and in certain circumstances, we might also process personal data about parents / carers, some of which might be sensitive personal data, information about criminal proceedings / convictions or information about child protection / safeguarding. This information is not routinely collected about parents / carers and is only likely to be processed by the school in specific circumstances relating to particular pupils, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

We collect information about parents / carers before pupils join the school and update it during pupils' time on the roll as and when new information is acquired.

Collecting parent / carer information

Whilst the majority of information about parents / carers provided to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain parent / carer information to us or if you have a choice in this. Where appropriate, we will ask parents / carers for consent to process personal data where there is no other lawful basis for processing it, for example where we wish to request voluntary contributions or share information with the BSA (Parent Teacher Association). Parents / carers may withdraw consent given in these circumstances at any time.

Our basis for using special category data

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your child's personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Storing parent / carer data:

A significant amount of personal data is stored electronically, for example, on our database, Arbor. Some information may also be stored in hard copy format. Data stored electronically may be saved on a (cloud) based system which may be hosted in a different country.

Personal data may be transferred to other countries if, for example, we are arranging a school trip to a different country. Appropriate steps will be taken to keep the data secure.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Data Retention Policy which is available from the school office. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

The school has adopted the Information Management Toolkit and Retention Schedule for Schools created by the IRMS (Information and Records Management Society) and adheres to its principles and guidance.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer a parent / carer we will retain and securely destroy your personal information in accordance with our data protection policy.

Who do we share parent / carer information with?

We routinely share parent / carer information with:

- Schools that pupils attend after leaving us;
- Our Local Authority, Hertfordshire County Council
- Arbor MIS, text and email communication service and school payment system
- Medical Tracker (accident and medical reporting system) There may be occasions when it is necessary to share parent / carer information other third parties including the following:
- Early Years Funding Portal
- Safeguarding and child protection professionals
- Disclosure and Barring Service
- CPOMS (Safeguarding reporting system)
- a new school where a child may be transferring
- a pupil's home local authority (if different);
- the Department for Education (DfE);
- school governors;
- the Police and law enforcement agencies;
- NHS health professionals including the school nurse, educational psychologists,
- Attendance Improvement Officers;
- Courts, if ordered to do so; • the Teaching Regulation Authority;

- Prevent teams in accordance with the Prevent Duty on schools;
- other schools, for example, if we are negotiating a managed move and we have your consent to share information in these circumstances;
- our legal advisors;
- our insurance providers

Some of the organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data. In the event that we share personal data about parents / carers with third parties, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

Requesting access to your personal data

Under data protection legislation, parents / carers have the right to request access to information about them that we hold ("Subject Access Request"). To make a request for your child's personal data, or be given access to your child's educational record, contact the Data Protection Officer via email admin@odbst.org although any written request for personal data will be treated as a Subject Access Request.

The legal timescales for the School to respond to a Subject Access Request is one calendar month. As the School has limited staff resources outside of term time, we encourage parents / carers to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible. For further information about how we handle Subject Access Requests, please see our Data Protection Policy.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of our data protection responsibilities.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing

and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the School Office (email: XXXXX). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Officer

We have appointed a data protection officer (DPO) to oversee compliance with this Privacy Notice. If you have any questions about this Privacy Notice or how we handle your personal information, please contact our DPO, Mrs Rachael Hollinshead via admin@odbst.org.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. You can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.uk/global/contactus/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

Changes to this Privacy Notice

We reserve the right to update this Privacy Notice at any time, and we will provide you with a new Privacy Notice when we make any substantial updates.

We may also notify you in other ways from time to time about the processing of your personal information.

Privacy notice on Pupil data for parents

Under data protection law, individuals have a right to be informed about how the trust/school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how the Trust, through its schools, collects, stores and uses personal data about **pupils**. This means that we collect and use personal information for specified purposes which this Privacy Notice has been designed to tell you about.

The Trust is the 'data controller' for the purposes of data protection law.

Our data protection officer and contact details are below (see 'Contact us' below).

Personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents, including emergency contacts, attainment records and assessment results
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information

- Free school meal and Pupil Premium eligibility
- Details of any medical information and dietary requirements, including physical and mental health
- Reported accidents
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

What is the purpose of us collecting and using pupil information?

The purposes for which the school collects personal information are as follows:

- To provide appropriate pastoral care
- To support with medical conditions, allergies and SEN
- To manage admissions
- To report and respond to safeguarding concerns
- To support pupil learning
- To provide school meals
- To Monitor and report on your progress and learning
- To ensure that you are safe when attending organised trips, participating in extracurricular activities and events.
- To promote the school and celebrate educational achievement
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations.

Please refer to ODBST's Records Management Policy.

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Our regulator e.g. Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies. We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013. To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:
- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data. For more information about the department's data sharing process, please visit: https://www.gov.uk/dataprotection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

https://www.gov.uk/government/publications/national-pupildatabase-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Schools with pupils aged 13 and above

Youth support services

Once our pupils reach the age of 13, we are legally required to pass on certain information about them to [name of local authority or youth support services provider in your area], as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to the relevant local authority or youth support service provider.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form
  Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

COVID-19 and Test and Trace

In the event that there is a case of COVID-19 in the school, alongside our protocols for dealing with such an event, there may be the possibility that we will be expected to provide limited contact information about some individuals to the NHS Test and Trace programme. This may include your details, subject to the circumstances at the time. Information will be processed in accordance with data protection legislation and the requirements of the NHS Test and Trace programme.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:

Data Protection Policy

ODBST Data Protection Officer
Oxford Diocesan Bucks Schools Trust
The Green
Longwick
Buckinghamshire
HP27 9QY

Email: admin@odbst.org

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

2. Privacy notice for pupils

You have a legal right to be informed about how our Trust uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.
We, the Trust, are the 'data controller' for the purposes of data protection law. This means that we collect and use personal information for specified purposes which this Privacy Notice has been designed to tell you about.

Our Data Protection Officer is listed below (see 'Contact us' below). The DPO is responsible for dealing with data protection issues within the Trust and you can contact the DPO should you wish to discuss any issues or concerns that you have about data protection.

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details, including emergency contacts
- Attainment records and assessment results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Free school meal and Pupil Premium eligibility
- Any medical information and dietary requirements you have
- Reported accidents
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

What is the purpose of us collecting and using pupil information

The purposes for which the school collects personal information are as follows:-

- To provide appropriate pastoral care
- To support your with medical conditions, allergies and SEN
- To manage admissions
- To report and respond to safeguarding concerns
- To support your learning
- To provide school meals
- To Monitor and report on your progress and learning
- To ensure that you are safe when attending organised trips, participating in extracurricular activities and events.

- To promote the school and celebrate educational achievement

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
  - Check how you're doing in exams and work out whether you or your teachers need any extra help
  - Track how well the school as a whole is performing
  - Look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.
Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.

Our Records Management Policy sets out how long we must keep information about pupils.

Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – to meet our legal duties to share certain information with it, such as concerns about pupils' safety and exclusions
- The Department for Education (a government department)

- Your family and representatives
- Educators and examining bodies
- Our regulator (the organisation or "watchdog" that supervises us),e.g. Ofsted
- Suppliers and service providers – so that they can provide the services we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies. We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013. To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

• conducting research or analysis

• producing statistics

• providing information, advice or guidance the Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

• who is requesting the data

• the purpose for which it is required

• the level and sensitivity of data requested: and

• the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data. For more information about the department's data sharing process, please visit: https://www.gov.uk/dataprotection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupildatabase-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Schools with pupils aged 13 years and over

Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to the relevant local authority as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Your parents/carers, or you once you're 16, can contact our data protection officer to ask us to only pass your name, address, and date of birth to the relevant local authority or local youth service provider.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

a. How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request, please contact our data protection officer.

b. Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)

- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting our data protection officer.

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

COVID-19 and Test and Trace

In the event that there is a case of COVID-19 in the school, alongside our protocols for dealing with such an event, there may be the possibility that we will be expected to provide limited contact information about some individuals to the NHS Test and Trace programme. This may include your details, subject to the circumstances at the time. Information will be processed in accordance with data protection legislation and the requirements of the NHS Test and Trace programme.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

ODBST Data Protection Officer
Oxford Diocesan Bucks Schools Trust
The Green
Longwick
Buckinghamshire
HP27 9QY
Email: admin@odbst.org

This notice is based on the Department for Education's model privacy notice for pupils, amended to reflect the way we use data in this trust.

3. Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the trust/school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how the Trust, through our schools, collects, stores and uses personal data about individuals we employ, or otherwise engage, to work at our school.

We, the Trust, are the 'data controller' for the purposes of data protection law. This means that we collect and use personal information for specified purposes which this Privacy Notice has been designed to tell you about.

Our Data Protection Officer is listed below (see 'Contact us' below). The DPO is responsible for dealing with data protection issues within the Trust and you can contact the DPO should you wish to discuss any issues or concerns that you have about data protection.

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school and Trust, including to:

- Enable you to be paid

- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our Records Management Policy.

Who do we share your data with and why

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- The Department for Education- underpins school funding and educational attainment policy and monitoring. We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under The Education (Information About Individual Pupils) (England) Regulations 2013.
- Your family or representatives
- Educators and examining bodies
- Our regulator e.g. Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Central and local government
- Multi-agency partners
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

a. How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

COVID-19 and Test and Trace

In the event that there is a case of COVID-19 in the school, alongside our protocols for dealing with such an event, there may be the possibility that we will be expected to provide limited contact information about some individuals to the NHS Test and Trace programme. This may include your details, subject to the circumstances at the time. Information will be processed in accordance with data protection legislation and the requirements of the NHS Test and Trace programme.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:

- ODBST Data Protection Officer
  Oxford Diocesan Bucks Schools Trust
  The Green
  Longwick
  Buckinghamshire
  HP27 9QY
  Email: admin@odbst.org

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this trust.

4. Job Applicant Privacy notice

Introduction

The Oxford Diocesan Bucks Schools Trust (ODBST) has several obligations under the General Data Protection Regulation (GDPR). This privacy notice sets out the types of data we hold on you as an employee of ODBST and how we use and store that information when you apply to work for us, during the recruitment process and subsequently if you become an employee of ODBST.

Data Controller Details

ODBST is the data controller for all its member schools and its central team. Our postal address is Oxford Diocesan Bucks School Trust, The Green, Longwick, Buckinghamshire, HP27 9QY.

The Data Protection Officer for ODBST can be contacted at: admin@odbst.org.

Data Protection Principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way;
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you;
- only use it in the way that we have told you about;
- ensure it is correct and up to date;
- keep your data for only as long as we need it;
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed.

Types of data we process

We process personal data for employment purposes to assist in the running of ODBST.

This personal data includes, but is not restricted to:

- Your name, date of birth, address, telephone number/s and email address, emergency contacts
- Details of qualifications, skills, experience, employment history, other relevant
- experience, professional memberships and achievements
- Information about your current remuneration level, including benefit entitlements
- Proof of your right to work in the UK
- Whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process

- Equality monitoring information, including information about your gender, ethnic origin, sexual orientation, age, health and religion or belief
- Employment references and the results of any pre-employment screening i.e. DBS checks or fitness to work
- The outcome and results of any interviews or tests which formed part of the recruitment process
- Bank account details, National Insurance number and tax status information
- Copy of driving licence
- Photographs used during a recruitment exercise and for building access passes

We collect data about you in a variety of ways and this will usually start during a recruitment exercise, such as an application form completed by you and interview notes made on behalf of ODBST. In some cases, we may also collect data from third parties such as when taking up references from former employers. Personal data is kept in paper personnel files within Schools or within ODBST's electronic HR and IT systems, depending on the role applied for. This information is kept secure and is only used for purposes directly relevant to your employment.

How ODBST process your data

The purpose of processing this data is to help us run the Trust, including to:

- Make an offer of employment to successful candidates
- Process data in order to enter into an employment contract
- To ensure legal obligations are fulfilled, i.e. checking proof of right to work in the UK before employment commences and seeking information regarding criminal convictions and offences
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Defend any legal claims
- Determine whether we need to make any reasonable adjustments to the recruitment process for candidates who have a disability
- For equality monitoring purposes
- Inform our recruitment and retention policies

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment contract that we are party to;
- in order to carry out legally required duties;
- in order for us to carry out our legitimate interests;
- to protect your interests; and
- where something is done in the public interest.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data.

By way of example, the personal data that is provided by you, or requested from you, during a recruitment process will enable us to perform the employment contract that we are party to (e.g. pay you), carry out our legally required duties (e.g. ensure you have the right to work in the UK) and carry out our legitimate interests (e.g. ensure that in line with safeguarding procedures the appropriate checks have been made before you commence employment with us). Any data that is collected to adhere to the various safeguarding requirements in schools also has a pupil, and public, interest angle.

When we collect personal information on our forms, we will make it clear whether there is a legal requirement for you to provide it, and whether there is a legal requirement on the Trust to collect it. If there is no legal requirement then we will explain why we need it and what the consequences are if it is not provided.

How ODBST share your information with third parties

We will not share information about you with third parties without your consent unless the law allows us to.

We are required, by law, to pass on some of the personal data which we collect to:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- The Department for Education
- Police forces
- Professional bodies
- Employment and recruitment agencies

This list is not exhaustive but indicates the key organisations your information may be shared with.

If you require more information about how the Trust, local authority and / or DfE store and use your personal data please visit:

- https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

Other organisations with whom we may share your personal data include:

- The Disclosure and Barring Service for the purposes of carrying out checks on your suitability for work with children;
- Our payroll provider- e.g. national insurance number and bank account details- to enable you to be paid;
- HMRC in conjunction with your legal obligation to pay income tax and make national insurance contributions;
- Our staff absence insurance company
- Our Fitness to Work and our Occupational Health provider
- A child-care voucher provider where you have decided to become part of that scheme so that they can provide the vouchers to you;
- A pension provider, such as Teachers' Pensions or the Local Government Pension Scheme in order to make sure that you pay the correct amount and maintain your entitlement to a pension upon your retirement. To see their privacy policies please visit:
    - http://www.tpt.org.uk/privacy-policy
    - https://www.buckscc.gov.uk/services/council-and-democracy/privacy-policy/

Our disclosures to third parties are lawful because one of the following reasons applies:

- The disclosure is necessary for the performance of your employment contract;
- The disclosure is necessary for the performance of a legal obligation to which ODBST is subject, for example our legal duty to safeguard pupils;

- The disclosure is necessary to protect the vital interests of others, i.e. to protect pupils from harm;
- The disclosure is necessary for the performance of our education function which is a function in the public interest.

We do not share your data with bodies outside of the European Economic Area.

How long we keep your personal information

The information you provide as part of your application will be used in the recruitment process. We will hold your data securely with access restricted to those involved in dealing with your application and in the recruitment process. Once this process is completed the data relating to unsuccessful applicants will be destroyed/deleted after 6 months. If you are the successful candidate, your application form and supporting documents, including references, DBS record and Fitness to Work confirmation, will be retained to form the basis of your personnel record with the Trust.

Your rights

You have a number of rights relating to data we hold about you. These include the right to:

- Ask for access to your personal information;
- Ask for rectification of the information we hold about you;
- Ask for the erasure of information about you;
- Ask for our processing of your personal information to be restricted;
- Data portability (in some cases you can ask the Trust to send you an electronic copy of your data so that it can be given to somebody else);
- Object to us using your information;
- Ask the Trust to stop processing your data for a period of time if data is inaccurate or if you have a dispute about whether or not your interests override the Trust's legitimate grounds for processing data;
- Ask the Trust to explain to you the logic behind any automated decision making, including profiling, based on your data.

More information about your rights is available in our Data Protection Policy, available from the Trust's Data Protection Officer.

Automated decision-making

The Trust's recruitment processes are not based solely on automated decision-making.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the organisation during the recruitment process. However, if you do not provide the information requested as part of the Trust's requirements, then the Trust may not be able to process your application as we will be unable to process the data needed to do so.

Information Commissioners Contact Information

If at any time you are not happy with how we are processing your personal information then you may raise the issue with the ODBST Data Protection Officer. If you are not happy with the outcome you may raise a complaint with the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

COVID-19 and Test and Trace

In the event that there is a case of COVID-19 in the school, alongside our protocols for dealing with such an event, there may be the possibility that we will be expected to provide limited contact information about some individuals to the NHS Test and Trace programme. This may include your details, subject to the circumstances at the time. Information will be processed in accordance with data protection legislation and the requirements of the NHS Test and Trace programme.

Updates to the ODBST Job Applicant Privacy notice

We reserve the right to update this privacy notice at any time, and we will provide candidates with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.